abblix

OIDC Server

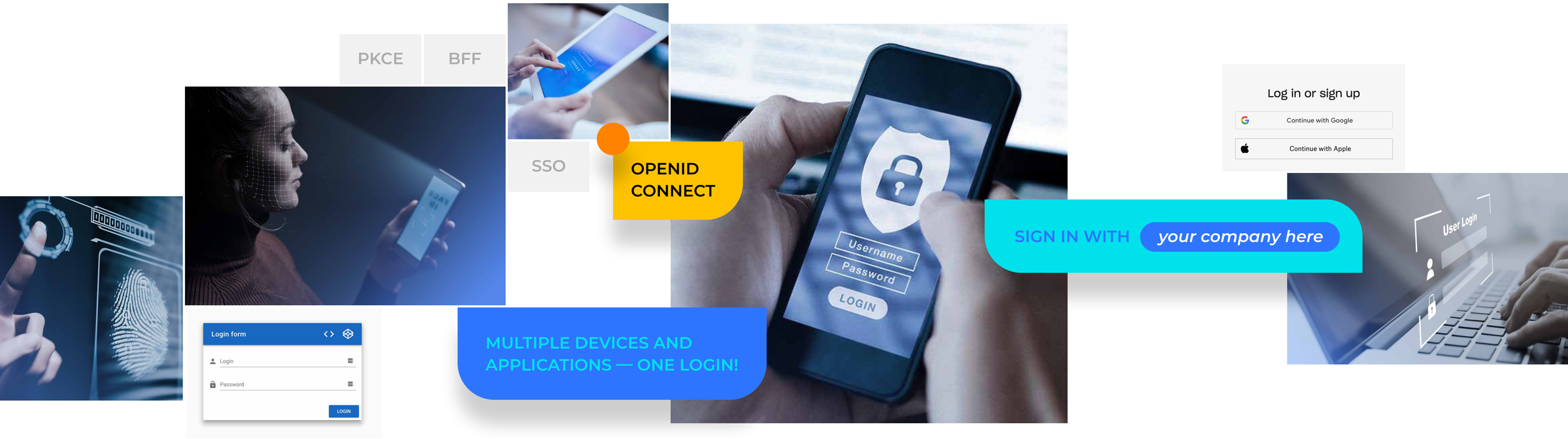
IMPLEMENTATION OF OPENID CONNECT AND OAUTH 2.0 FOR MODERN PROJECTS IN ASP.NET

For companies valuing full
control over authentication

ARE YOU PLANNING TO IMPLEMENT A MODERN AUTHENTICATION SYSTEM?

DO YOU NEED A RELIABLE AND SECURE SINGLE SIGN-ON (SSO) SYSTEM?

ARE YOU PLANNING TO CREATE YOUR OWN IDENTITY PROVIDER?



WE KNOW HOW TO SOLVE THIS TASK AND WILL HELP YOU WITH IT!

WHY IS THE **OPENID CONNECT** PROTOCOL THE BEST SOLUTION FOR AUTHENTICATION?

MODERN STANDARD AND BROAD SUPPORT

Unlike outdated and insecure protocols like OAuth 1.0, SAML, and WS-Federation, OpenID Connect is the most advanced and popular authentication standard, supported by numerous libraries and tools. It is the de facto standard in 2024.

FLEXIBILITY

It allows for easy addition of new domains and adaptation to changes in architecture without significant time and resource costs. This ensures scalability and long-term sustainability of solutions.

COMPATIBILITY

Easily integrates with existing systems, allowing for a seamless implementation of OpenID Connect into your infrastructure.

SECURITY AND SEPARATION OF CONCERNS

Provides reliable data protection and prevents unauthorized access. It separates user authentication processes from resource management, enhancing overall system security.

MOBILE AND WEB APPLICATIONS

Provides a universal authentication mechanism for various platforms, such as web applications, mobile apps, smart TV apps, and more.

WHY IS A **SERVER LIBRARY** BETTER THAN A CLOUD OR BOXED SOLUTION?

DATA CONTROL AND LEGAL COMPLIANCE

You decide where and how your data is stored. You control the storage format, backup, and data placement, including the choice of data centers and regions. Full control over user data helps ensure security and privacy. It also simplifies compliance with local and international regulations, such as GDPR and HIPAA, since the data remains within your infrastructure.

INTEGRATION AND CUSTOMIZATION FLEXIBILITY

You can integrate the server library into your existing architecture, retaining your user database, authentication forms (UI), and current connections with other systems. The library allows for complete customization to meet your requirements, including any authentication factors: one-time passwords (OTP), biometrics, hardware keys, and their combinations. If you already have an account database, UI, or authentication service without OpenID Connect support, our solution will easily enable its integration.

NO VENDOR LOCK-IN

Relying on cloud solutions can lead to challenges, when there is a need to move data to another provider or to your own data center. Data export can be difficult or impossible, risking data loss. By using your own solution with the OpenID Connect library, you avoid these risks. You maintain full control over your user base, independent of third-party providers and their policy changes, ensuring smooth transitions if you switch providers.

NO GEOPOLITICAL RISKS

The conflict between the US and China has led to restrictions on cloud services and support. Brexit introduced additional requirements for data exchange between the UK and the EU. Some services were disrupted due to sanctions and new laws. By relying on your own authentication service, you eliminate the risks of cloud solution unavailability or lack of technical support. User authentication remains fully under your control.

abblix

WHO WE ARE

Abblix, founded in 2022, brings together specialists with over a decade of experience in authentication and is focused on developing advanced solutions in this field.

MISSION

To provide best-in-class authentication solutions, ensuring reliability and ease of use for our clients.

COMPANY ABBLIX AND THE PRODUCT **OIDC SERVER**

OpenID CERTIFIED

astana hub

PRODUCT

OIDC Server is a server library implementing the OpenID Connect standard on the .NET platform. In addition to providing reliable and secure authentication, the library is characterized by its flexibility, ease of customization, and seamless integration into existing architecture.

ACHIEVEMENTS

- Abblix LLP is a resident of Astana Hub, the largest IT park in Central Asia.
- OIDC Server has successfully passed official certification by the OpenID Foundation for all key profiles, confirming its high reliability and full compliance with standards.

WHY CHOOSE **OIDC SERVER**?

CERTIFICATION AND SECURITY

The OIDC Server library is certified by the OpenID Foundation for all profiles. This ensures full compliance with standards for reliable and secure authentication.

EASY INTEGRATION AND FLEXIBLE ARCHITECTURE

The library is ready to use with ASP.NET Core: standard controllers, data binding, and routing are all available out of the box. However, thanks to its hexagonal architecture, you can easily adapt and integrate the abstract core of the library into any existing or future frameworks for creating a Web API implementing the OpenID Connect protocol.

MODULAR DESIGN AND OPEN SOURCE

The library is initially designed with a focus on ease of extension. We have separated the stages of validation, request processing, and response formatting, and supported library configuration through the standard .NET dependency injection mechanism. By applying well-known design patterns, you can easily add or modify virtually any aspect of the library's behavior to meet various project requirements. The source code is available on GitHub, ensuring development transparency and third-party security audits.

CROSS-PLATFORM AND .NET SUPPORT

The code is developed for the popular .NET platform, ensuring high compatibility and performance. The library runs on Windows and Linux servers, is compatible with Docker and Kubernetes, which simplifies deployment and scaling management.

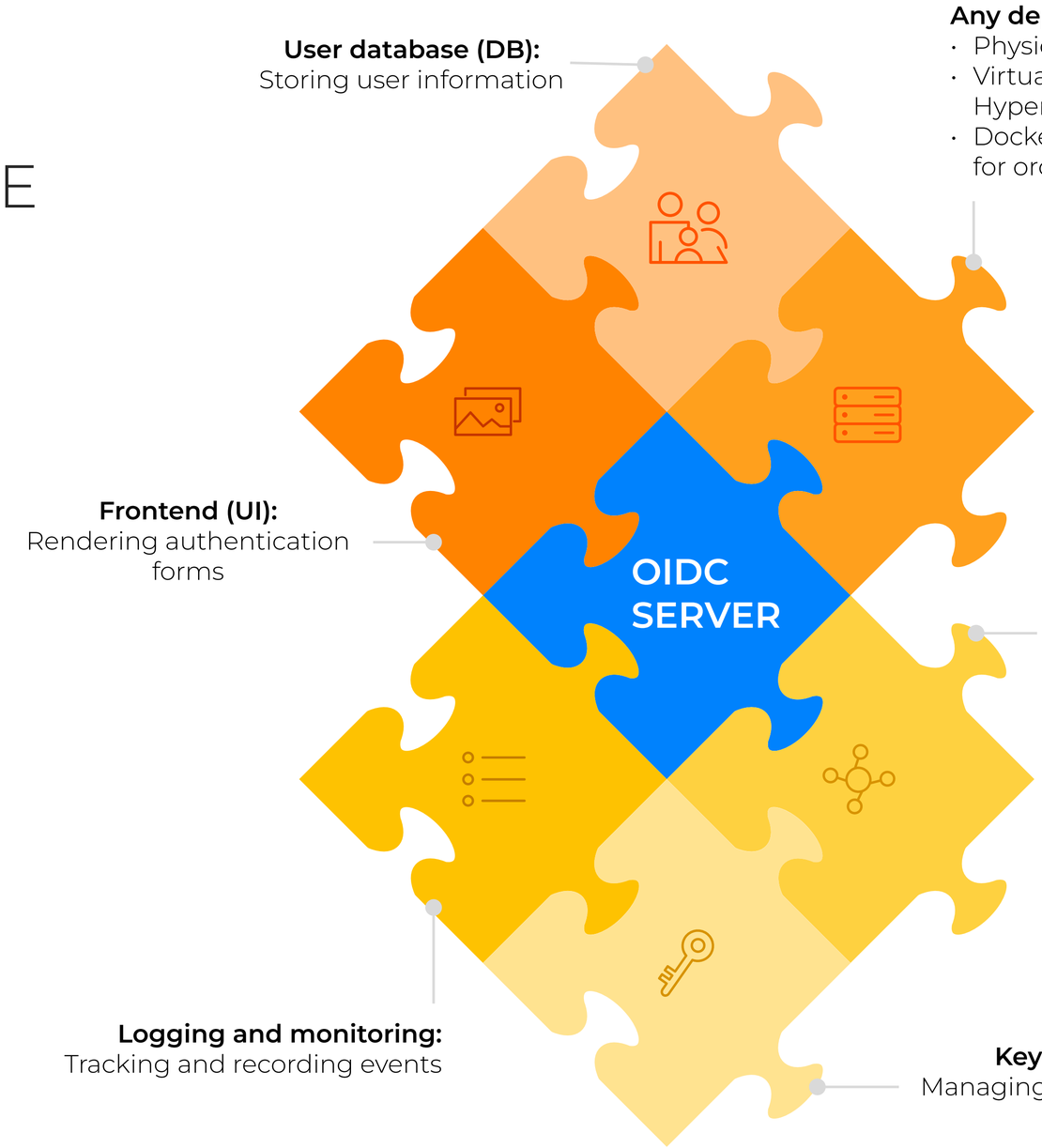
OIDC SERVER
IN YOUR INFRASTRUCTURE

Abblix's responsibility:

STRICT COMPLIANCE WITH THE OPENID CONNECT STANDARD

EVERYTHING ELSE IS YOUR RESPONSIBILITY

We offer exceptional flexibility both when implementing the system from scratch and when upgrading an existing one. In the case of an upgrade, you can maximize the reuse of existing functionality, including authentication UI forms, key storage systems, logging, and user information databases.



User database (DB):
Storing user information

Any deployment options:
- Physical server
- Virtual server (e.g., VMWare, Hyper-V)
- Docker container (with Kubernetes for orchestration)

Frontend (UI):
Rendering authentication forms

API and services:
Integration with external and internal systems

Logging and monitoring:
Tracking and recording events

Key Storage:
Managing cryptographic keys

TECHNICAL REQUIREMENTS AND IMPLEMENTED STANDARDS FOR **OIDC SERVER**

SUPPORTED PLATFORMS

Runs on .NET-compatible platforms. Supports .NET 6.0, .NET 7.0, and .NET 8.0.

WEB SERVER REQUIREMENTS

Any compatible web server, including:
Nginx
Apache HTTP Server
Microsoft IIS

HARDWARE REQUIREMENTS

No specific hardware requirements are needed. System performance and memory capacity should effectively scale according to the operational loads of the system.

IMPLEMENTED TECHNOLOGIES AND STANDARDS

The OAuth 2.0 Authorization Framework: RFC 6749: Defines procedures for secure authorization of applications.
The OAuth 2.0 Authorization Framework: Bearer Token Usage: RFC 6750: Explains how to securely use bearer tokens to access resources.
OAuth 2.0 Token Revocation: RFC 7009: Describes methods to securely cancel access and refresh tokens.
OAuth 2.0 Dynamic Client Registration Protocol: RFC 7591: Provides mechanisms for clients to register dynamically with authorization servers.
Proof Key for Code Exchange by OAuth Public Clients: RFC 7636: Improves security for public clients during authorization code exchange.
OAuth 2.0 Token Introspection: RFC 7662: Allows resource servers to verify the active state and metadata of tokens.
OAuth 2.0 Token Exchange: RFC 8693: Details the method for a secure exchange of one token type for another.
OAuth 2.0 Resource Indicators: RFC 8707: Enables users to specify the resources they want access to, enhancing security and access control.
JSON Web Token (JWT): RFC 7519: Defines structure and use of JWTs for representing claims securely.
JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants: RFC 7523: Uses JWTs for secure client authentication and as authorization grants.
JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens: RFC 9068: Specifies the use of JWTs as OAuth 2.0 access tokens.
The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR): RFC 9101: Secures authorization requests using JWTs.
OAuth 2.0 Pushed Authorization Requests: RFC 9126: Enhances security by allowing clients to push authorization requests directly to the server.
OAuth 2.0 Authorization Server Issuer Identification: RFC 9207: Ensures the authenticity of authorization servers to clients.
OAuth 2.0 Multiple Response Type Encoding Practices: Core Specification: Encodes different response types in OAuth 2.0 requests.
OAuth 2.0 Form Post Response Mode: Core Specification: Transmits OAuth 2.0 responses via HTTP form posts.
OpenID Connect Core: Core Specification: Core functionality for OpenID Connect identity layer over OAuth 2.0.
OpenID Connect Core: Pairwise Pseudonymous Identifiers (PPID): Core Specification: Implements a privacy mechanism by generating unique identifiers for clients.
OpenID Connect Discovery: Detailed Specification: Enables clients to discover provider configurations dynamically.
OpenID Connect Dynamic Client Registration: Detailed Specification: Enables OpenID Connect clients to register dynamically with providers.
OpenID Connect RP-Initiated Logout: Detailed Specification: Details logout initiated by relying parties.
OpenID Connect Session Management: Detailed Specification: Manages user session states in identity providers.
OpenID Connect Front-Channel Logout: Detailed Specification: Handles logout requests through front-channel communication.
OpenID Connect Back-Channel Logout: Detailed Specification: Manages logout processes using back-channel communication.

PRICING POLICY

We offer flexible pricing plans suitable for businesses of any size

CLIENT APPLICATIONS
Software applications registered to interact with the OpenID Connect server for authentication and token generation.

ISSUERS
Unique authorization servers in OpenID Connect that can combine multiple servers for load balancing and failover, using a single URL.

NOT-FOR-PROFIT USE?
THE PRODUCT IS FREE FOR YOU!

DIDN'T FIND A PRICING PLAN THAT FULLY MEETS YOUR NEEDS?

Contact us, and we'll find a solution that works for you!

abblix

STARTER	BUSINESS	ENTERPRISE
Ideal for small businesses or individual developers	For growing businesses and developer teams	For large enterprises with extensive development needs
Client applications: **up to 5** (upgradable to 10 for $300 per additional client)	**Client applications:** **up to 15** (upgradable to 30 for $300 per additional client)	**Client applications:** **Unlimited**
Issuers: 1 (not upgradable)	**Issuers: 1** (not upgradable)	**Issuers:** **Unlimited**
Support: **Standard** (not upgradable)	**Support:** **Standard** (upgradable to Extended for $1,200)	**Support:** **Extended**
		Advanced features: · Dynamic client registration · Pairwise Identifiers (PPID) · Resource Indicators · Client Initiated Backchannel Authentication (CIBA) · Device authorization
$ 1,500 / YEAR	$ 4,500 / YEAR	$ 15,000 / YEAR

e: info@abblix.com

w: www.abblix.com

GitHub: github.com/Abblix/Oidc.Server

LinkedIn: linkedin.com/company/abblix

IF YOU HAVE ANY QUESTIONS AFTER READING THIS PRESENTATION, DON'T HESITATE TO CONTACT US!

We will be happy to answer all your questions and provide the necessary information.